Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 685 – 689

Procedia Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

A Study of Anonymous Purchasing Based on Mobile Payment System

Jieling Wu[a], Chenglian Liu[b,*], Donald Gardner[a]

[a]*Department of Economics and Management, Huizhou University, Huizhou 516007, China*
[b]*Department of Computer Science, Huizhou University, Huizhou 516007, China*

Abstract

"Anonymous purchasing" has been in use for about a decade. While we have been able to use anonymous purchasing to buy goods and services from home based desk-top computers for many years, it has only been within the last few years that anonymous purchasing has been used on a mobile platform. This has enabled the buyer to use anonymous purchasing almost anywhere such as restaurants where it had not been possible before. Now shoppers can easily use their Wechat account for purchasing goods using their mobile phone and do it anonymously. This has added to the privacy and security of the purchaser. This anonymity in purchasing is increasingly being demanded by more people. In this paper the authors will examine an anonymous purchasing system using digital signature techniques of cryptographic and mobile payment systems.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Digital Signature; Anonymous; Hash Function; Mobile Payment;

1. Introduction

Many young people in China purchase goods and services online from popular websites such as meituan.com, lashou.com, and diaping.com. On these websites, shoppers can purchase goods, services, entertainment and travel. In the past, when shoppers made purchases on the internet, they would usually use a credit or debit card, which obviously, has no anonymity. For some people this is fine, but a growing number of customers are demanding anonymous purchasing because of spam and other security issues. More recently, shoppers are making purchases using e-cash through "Wechat" (or the Chinese application "Weixin"). Wechat is an instant mobile messaging application that is a Location Based Service (LBS) technology which provides a function called "Searching for the nearby". These applications have obvious privacy threats because users may send personal information to everyone surrounding them through the wifi system. In this paper, the authors will examine an anonymous payment system, using a mobile payment platform such as Wechat, where three entities are used to keep the buyer anonymous and keep the information secret: the purchaser, merchant, and issuer (usually the bank). These three entities are combined using verification

* Corresponding author. Tel.: +86-18850899538.
E-mail address: chenglian.liu@gmail.com

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.152

codes, in such a way, as to keep the buyer' information secret. Wechat, and other mobile systems, have been studied by Gao and Ying on the iPhone[1]. Lien and Cao[2] studied how shoppers use Wechat in China. Mao[3] did a more detailed study of purchasing patterns of Chinese undergraduate students using WeChat. There is some related literature about mobile payment systems in[4,5,6,7], but they are out of the scope of this article.

2. Analysis of Three Player Anonymous E-Cash Systems

2.1. System Overview

This purchasing system operates as follows: 1) Buyer transfers his cash to issuer (bank). 2) Issuer (bank) sends receipt of cash to buyer. 3) Buyer uses e-cash in shop. 4) Seller checks the verification code by issuer (bank). 5) Issuer transfers e-cash to shop. 6) Seller confirms this transaction with buyer.

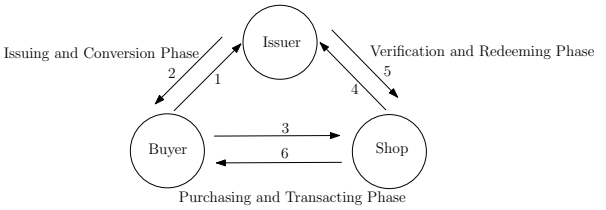

Figure 1. The role of three parties

2.2. Security Issues

Why would a shopper choose anonymous purchasing? The following are some important reasons: 1) To prevent the seller from collecting user data through transaction software such as the website. 2) It is confidential to purchaser. 3) To prevent advertising harassment. The main advantage of the system is that consumers remain anonymous because they do not send any personal information over wifi or other public systems.

3. Our Methodology and Scheme

There are seven phases in our methodology: system initialization, e-cash conversion, fetching, purchasing, verification, redemption and transaction confirmation. The following notations are used in this section:
Notations:
p: a large prime number where $|p|$ is 1204 bits length.
g: an element primitive generator of $\mathbb{Z}_p^*$.
x_i: the secret key.
y_i: the public key.
$h(.)$: a one-way hash function.
t: the e-cash.
m: money amount.
$||$: concatenation. These phases are described in the following subsection.

3.1. System Initialization

During system initialization, the buyer randomly chooses a secret key x_a to compute the public key y_a; the seller also randomly choose a secret key x_b to compute the public key y_b; the issuer randomly choose a secret key x_c to

compute the public key y_c, where

$$y_a \equiv g^{x_a} \pmod{p}, \tag{1}$$

$$y_b \equiv g^{x_b} \pmod{p}, \tag{2}$$

$$y_c \equiv g^{x_c} \pmod{p}. \tag{3}$$

The issuer agrees to share a secret parameter $h(m||t)$ with the seller. The $h(m||t)$ stores the money format and amount. See Figure 2.

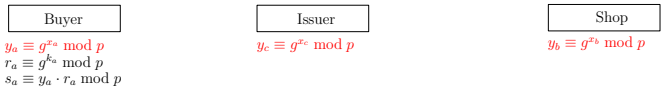

Figure 2. System Initialization Phase

3.2. Money Conversion

If the buyer wants to convert money to e-cash, k_a is randomly selected to find

$$r_a \equiv g^{k_a} \pmod{p} \tag{4}$$

$$s_a \equiv y_a \cdot r_a \pmod{p}. \tag{5}$$

s_a is sent to the issuer, see Figure 3.

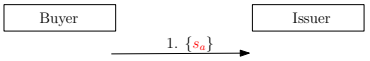

Figure 3. Money Conversion Phase

3.3. E-cash Fetching Phase

The issuer receives s_a (money) from buyer. A secret key x_c is used to compute T, where

$$T \equiv s_a^{x_c} \cdot h(m||t) \pmod{p}, \tag{6}$$

and feedback e-cash (T) to the buyer. When the buyer receives the e-cash (T), it is stored in the mobile device, see Figure 4.

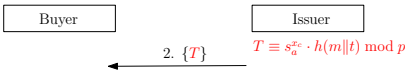

Figure 4. E-cash fetching phase

3.4. E-cash Using Phase

Upon receiving T, the buyer can use his e-cash to buy something from the merchant. Note: The buyer must keep the T. It is usually stored in the mobile phone or computer. In practice, the T is a voucher code, serial code or an electronic record, see Figure 5.

3.5. E-cash Verification Phase

When the shop obtains e-cash (T) from the buyer, the shop can check the validation code. The seller uses the secret key x_b to compute

$$T' \equiv (T)^{x_b} \cdot h(m||t)^{-x_b} \pmod{p}, \tag{7}$$

and sends T' to issuer, see Figure 6.

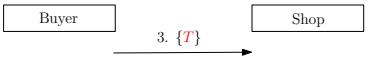

Figure 5. E-cash using phase

Figure 6. E-cash verification phase

3.6. Money Redeeming Phase

Issuer receives serial code T' to verify e-cash from seller, shop used x_c^{-1} to find verified serial code T'' where:

$$T'' \equiv (T')^{x_c^{-1}} \pmod{p}. \tag{8}$$

Issuer returns verified serial code T'' to seller. If verified, the sellers and buyers are legal users, see Figure 7.

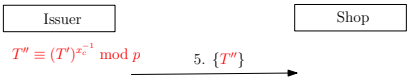

Figure 7. Money redeeming phase

3.7. Transaction Confirming Phase

Seller receives verified serial code T'' from issuer, seller used x_b^{-1} to find

$$T''' \equiv (T'')^{x_b^{-1}} \pmod{p}, \tag{9}$$

and then returns receipt T''' to buyer. Upon on receiving T''', buyer can verify

$$s_a \stackrel{?}{\equiv} T''' \pmod{p}, \tag{10}$$

If it is verified, the transaction is completed, see Figure 8.

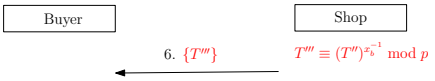

Figure 8. Transaction confirming phase

Proof.

$$\begin{aligned} s'_a &\stackrel{?}{\equiv} T''' \bmod p \\ &\equiv [T'']^{x_b^{-1}} \bmod p \\ &\equiv [[T']^{x_c^{-1}}]^{x_b^{-1}} \bmod p \\ &\equiv [[(T)^{x_b} \cdot h(m||t)^{-x_b}]^{x_c^{-1}}]^{x_b^{-1}} \bmod p \\ &\equiv [[((y_a \cdot r_a)^{x_c} \cdot h(m||t))^{x_b} \cdot h(m||t)^{-x_b}]^{x_c^{-1}}]^{x_b^{-1}} \bmod p \\ &\equiv s_a \bmod p. \end{aligned} \tag{11}$$

□

The detailed scheme shows on Figure 9.

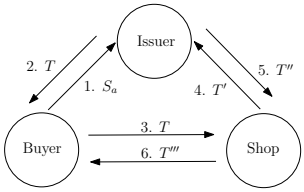

Figure 9. The progress of our scheme

3.8. Security Analysis

The purchaser's information is anonymous when the system uses a one-way hash function[8], this function has several properties, two of which are pre-image resistance and collision resistance.

Scenario 1: If attacker wants to find the x_a or k_a from the known y_a or r_a, modulus p and generator g, he would challenge the discrete logarithm problem.

Scenario 2: Only buyer compute y_a since he owns his secret key x_a, where $y_a \equiv g^{x_a} \pmod{p}$, even if the s_a and the y_a are published, anybody may find $r_a \equiv y_a^{-1} \cdot s_a \pmod{p}$ by Equation (5). Buyer transferred his e-cash upon on the s_a to T since s_a be linked to y_a and r_a; buyer just announced his y_a, he does not publish r_a. Hence, no one can trace and modify any information, the buyer's identity is still anonymity.

Scenario 3: The issuer can not deny his identifier behavior by Equation (6). The issuer signed s_a using his private key x_c and a secret share parameter $h(m||t)$ to obtain the warrant T. Namely, the voucher code or verification code.

Scenario 4: The seller can not mutually deny his action. Since T' is produced by the shop, although the seller does not know x_c and s_a, but he could use x_b to find T' and return to issuer. If T' is incorrect, the issuer can not recovery T'' from T'. Therefore, the seller and issuer also can not deny each others. See Equation (7) and Equation (8).

4. Conclusion

In this paper the authors have proposed a scheme to provide security for a mobile purchaser so that the consumer does not have to be concerned about leaking any sensitive data on a public network. On a mobile purchasing system, users usually store the serial code T (cash) in their mobile phone, which presents a security problem. We solved this problem by the use of serial and verification codes thus improving the efficiency and security of the mobile anonymous system.

Acknowledgments

The authors would like to thank the anonymous reviewers for their useful comments. This work is partially supported from Huizhou University project under the number HZUX1201418.

References

1. Gao, F., Zhang, Y.. Analysis of wechat on iphone. In: *2nd International Symposium on Computer, Communication, Control and Automation*. 2013, p. 278–281.
2. Lien, C.H., Cao, Y.. Examining wechat users' motivations, trust, attitudes, and positive word-of-mouth: Evidence from china. *Computers in Human Behavior* 2014;**41**:104–111.
3. Mao, C.. Friends and relaxation: Key factors of undergraduate students' wechat using. *Creative Education*, 2014;**5**:636–640.
4. Put, A., Dacosta, I., Milutinovic, M., De Decker, B., Seys, S., Boukayoua, F., et al. inshopnito: An advanced yet privacy-friendly mobile shopping application. In: , *2014 IEEE World Congress on Services (SERVICES)*. 2014, p. 129–136. doi:10.1109/SERVICES.2014.32.
5. Yang, B., Feng, D., Qin, Y.. A lightweight anonymous mobile shopping scheme based on daa for trusted mobile platform. In: *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. 2014, p. 9–17.
6. Liu, C., Wu, J.. Study of anonymous delivery system using proxy blind signature scheme. In: *2015 17th UKSIM-AMSS International Conference on Modelling and Simulation*. ISBN 978-1-4799-8713-9/15; 2015, p. 223–226.
7. Wu, J., Liu, C.. A study of anonymous delivery based on blind signature scheme. *Procedia Computer Science* 2015;**52**:1065–1070.
8. Wikipedia, . Cryptographic hash function. http://en.wikipedia.org/wiki/Cryptographic_hash_function; 2015.